

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平7-36672

(43)公開日 平成7年(1995)2月7日

(51)Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 7/58	C			
G 0 9 C 1/00		8837-5L		
H 0 4 L 9/22				

H 0 4 L 9/ 04

審査請求 未請求 請求項の数6 O L (全 12 頁)

(21)出願番号 特願平5-179232

(22)出願日 平成5年(1993)7月20日

(71)出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72)発明者 山本 貴久

東京都大田区下丸子3丁目30番2号キヤノン株式会社内

(72)発明者 岩村 恵市

東京都大田区下丸子3丁目30番2号キヤノン株式会社内

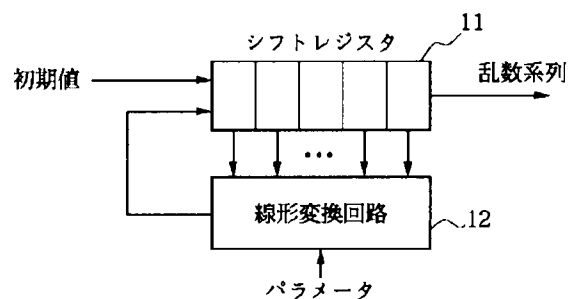
(74)代理人 弁理士 丸島 儀一

(54)【発明の名称】 乱数発生器、及びそれを用いた通信システム及びその方法

(57)【要約】

【目的】 高速かつ安全な乱数系列を発生する。

【構成】 データを保持するシフトレジスタ11と、該シフトレジスタ11に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する線形変換回路12と、該線形変換回路12による変換結果に基づき、前記シフトレジスタ11に保持されるデータを更新する更新手段と、前記シフトレジスタ11に保持されるデータの一部を、乱数系列として順次出力する出力手段とを具える。



## 【特許請求の範囲】

【請求項 1】 データを保持する保持手段と、  
該保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する変換手段と、  
該変換手段による変換結果に基づき、前記保持手段に保持されるデータを更新する更新手段と、  
前記保持手段に保持されるデータの一部を、乱数系列として順次出力する出力手段とを具え、前記パラメータを所定の周期で変更することを特徴とする乱数発生器。

【請求項 2】 データを保持する保持手段と、  
該保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する変換手段と、  
該変換手段による変換結果に基づき、前記保持手段に保持されるデータを更新する更新手段と、  
前記保持手段に保持されるデータの一部を、乱数系列として順次出力する出力手段と、  
前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する算出手段とを具えることを特徴とする乱数発生器。

【請求項 3】 データを保持する第 1 の保持手段と、  
該第 1 の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第 1 の変換手段と、  
該第 1 の変換手段による変換結果に基づき、前記第 1 の保持手段に保持されるデータを更新する第 1 の更新手段と、  
前記第 1 の保持手段に保持されるデータの一部を、乱数系列として順次出力する第 1 の出力手段と、  
該第 1 の出力手段より出力される乱数系列に基づいて通信文を暗号化する暗号化手段とを送信装置に具え、  
データを保持する第 2 の保持手段と、  
該第 2 の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第 2 の変換手段と、  
該第 2 の変換手段による変換結果に基づき、前記第 2 の保持手段に保持されるデータを更新する第 2 の更新手段と、  
前記第 2 の保持手段に保持されるデータの一部を、乱数系列として順次出力する第 2 の出力手段と、  
該第 2 の出力手段より出力される乱数系列に基づいて暗号文を復号する復号手段とを受信装置に具えたことを特徴とする通信システム。

【請求項 4】 データを保持する第 1 の保持手段と、  
該第 1 の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第 1 の変換手段と、  
該第 1 の変換手段による変換結果に基づき、前記第 1 の保持手段に保持されるデータを更新する第 1 の更新手段と、

前記第 1 の保持手段に保持されるデータの一部を、乱数系列として順次出力する第 1 の出力手段と、  
前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する第 1 の算出手段と、  
前記第 1 の出力手段より出力される乱数系列に基づいて通信文を暗号化する暗号化手段とを送信装置に備え、  
データを保持する第 2 の保持手段と、  
該第 2 の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第 2 の変換手段と、  
該第 2 の変換手段による変換結果に基づき、前記第 2 の保持手段に保持されるデータを更新する第 2 の更新手段と、  
前記第 2 の保持手段に保持されるデータの一部を、乱数系列として順次出力する第 2 の出力手段と、  
前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する第 2 の算出手段と、  
前記第 2 の出力手段より出力される乱数系列に基づいて暗号文を復号する復号手段とを受信装置に具えたことを特徴とする通信システム。

【請求項 5】 送信側で、データを保持する第 1 の保持部に保持されたデータを第 1 の変換部に入力し、  
所定のパラメータに基づいて入力データを変換し、  
該変換の結果に基づき、前記第 1 の保持部に保持されるデータを更新し、  
前記第 1 の保持部に保持されるデータの一部を、乱数系列として順次出力し、  
該出力される乱数系列に基づいて通信文を暗号化して暗号文を順次受信側に送信し、  
受信側で、データを保持する第 2 の保持部に保持されたデータを第 2 の変換部に入力し、  
所定のパラメータに基づいて入力データを変換し、  
該変換の結果に基づき、前記第 2 の保持部に保持されるデータを更新し、  
前記第 2 の保持部に保持されるデータの一部を、乱数系列として順次出力し、  
該出力される乱数系列に基づいて暗号文を復号することを特徴とする通信方法。

【請求項 6】 送信側で、データを保持する第 1 の保持部に保持されたデータを第 1 の変換部に入力し、  
所定のパラメータに基づいて入力データを変換し、  
該変換の結果に基づき、前記第 1 の保持部に保持されるデータを更新し、  
前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更し、  
前記第 1 の保持部に保持されるデータの一部を、乱数系列として順次出力し、

該出力される乱数系列に基づいて通信文を暗号化する暗号文を順時受信側に送信し、  
受信側で、データを保持する第2の保持部に保持されたデータを第2の変換部に入力し、  
所定のパラメータに基づいて入力データを変換し、  
該変換の結果に基づき、前記第2の保持部に保持されるデータを更新し、  
前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを更新し、  
前記第2の保持部に保持されるデータの一部を、乱数系列として順次出力し、  
該出力される乱数系列に基づいて暗号文を復号することを特徴とする通信方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は暗号化方式に関係し、特に暗号通信分野におけるデータの秘匿、発信者・着信者の認証、暗号鍵の共有、零知識証明プロトコル等に関するものである。また、モンテカルロシミュレーションなどの乱数を用いたシミュレーションに関するものである。

【0002】

【従来の技術】従来、乱数発生法の一つとして、文献「現代暗号理論」（池野、小山著、昭和61年発行、電子情報通信学会）の第69～72頁に示されているように、最大長周期系列（M系列）を発生する線形フィードバックシフトレジスタ（LFSR）を用いたものが知られている。

【0003】LFSR方式とは、図14に示すようにs段のシフトレジスタ $R(t) = (r_s(t), r_{s-1}(t), \dots, r_2(t), r_1(t))$ とタップ（引込線）列 $(h_s, h_{s-1}, \dots, h_2, h_1)$ からなり、各時点（ストップ）ごとに次のような動作を同時に行うことにより、擬似乱数系列を生成する方法である。

【0004】(a) 最右端のレジスタのビット $r_1(t)$ を擬似乱数系列として出力する。

【0005】 $k_t = r_1(t)$

(b)  $r_s(t), r_{s-1}(t), \dots, r_2(t)$ を右にシフトする。

【0006】 $r_i(t+1) = r_{i+1}(t) \quad (i=1, 2, \dots, s-1)$

(c) 最左端のレジスタのビット $r_s(t+1)$ をレジスタの内容とタップ列により、次のように計算する。

【0007】

【外1】

$$r_s(t+1) = \sum_{i=1}^s h_i \cdot r_i(t) \bmod 2$$

以上まとめると、LFSR方式の擬似乱数発生アルゴリズムはs行s列の行列Hを用いて、

$$R(t+1) = H \cdot R(t) \bmod 2 \quad (1)$$

つまり、

【0008】

【外2】

$$\begin{bmatrix} r_s(t+1) \\ r_{s-1}(t+1) \\ r_{s-2}(t+1) \\ \vdots \\ r_2(t+1) \\ r_1(t+1) \end{bmatrix} = \begin{bmatrix} h_s & h_{s-1} & \dots & h_s & h_2 & h_1 \\ 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} r_s(t) \\ r_{s-1}(t) \\ r_{s-2}(t) \\ \vdots \\ r_2(t) \\ r_1(t) \end{bmatrix}$$

と表せる。

【0009】このs段のLFSRのタップ列をうまく選ぶと、最大周期 $2^s - 1$ の擬似乱数のビット系列を生成することができ、その時の系列が前述の最大長周期系列となる。

【0010】しかしながら、このLFSRを用いる乱数発生法では、LFSRの線形性を利用して2sビットの出力擬似乱数列からs段のタップ列 $(h_s, h_{s-1}, \dots, h_2, h_1)$ を以下の方法で決定できる。

【0011】出力される擬似乱数系列が $k_1, k_2, \dots, k_{2s}$ であったとすると、ある時点t ( $t=1, 2, \dots, s+1$ )のレジスタの内容 $R(t)$ は、  
 $R(1) = (k_s, k_{s-1}, \dots, k_1)^T$   
 $R(2) = (k_{s+1}, k_s, \dots, k_2)^T$   
 $\dots$

$R(s+1) = (k_{2s}, k_{2s-1}, \dots, k_{s+1})^T$ と表せる（ $^T$ は転置を示す）。この時、行列X、Yを  
 $X = (R(1), R(2), \dots, R(s))$   
 $Y = (R(2), R(3), \dots, R(s+1))$ とすると、式(1)より

$$Y = H \cdot X$$

の関係が成立するため、

$$H = Y \cdot X^{-1} \quad (2)$$

によりHが求められ、タップ列が決定される。

【0012】つまり、乱数の周期は $2^s - 1$ であるがそのうち2sビットでLFSRの構成が決定される。この場合、その時点以降に発生される乱数列が全てわかってしまうため、出力乱数列を暗号用の乱数として用いるには安全性の面で不適当であるという欠点があった。

【0013】また、非線形フィードバックシフトレジスタを用いれば、出力乱数系列の解析に必要な乱数の数を大きくすることができることが知られている。しかし、バーレカンブーマッセイのアルゴリズム（E. R. Berlekamp "Algebraic coding theory", McGraw-Hill Book Company, 1968）によりその系列を生成することができる最小段数のLFSRを求めることがで

き、非線形フィードバックシフトレジスタを用いた乱数発生方式も、式(2)の方法により解析される可能性があった。

【0014】以上の様に、ある時点までの出力乱数を手に入れることができれば、それ以降に出力する乱数列全てを容易に予測することができる乱数発生方式を便宜上方式Aと呼ぶことにする。方式Aは上述のように暗号学的に安全ではないが、構成が容易なので高速処理が可能であるという特徴を持つ。

【0015】方式Aとは異なり、ある時点までに発生させた乱数列のみからその時点以降に発生されるべき乱数を求めるための計算量は、 $n$ を因数分解するのに必要な計算量と同等であることが知られている。ただし、 $n$ を因数分解することを計算量的に困難にするためには $p$ 、 $q$ を数百ビット程度にする必要がある。このように、ある時点までに発生された乱数列のみからその時点以降に発生されるべき乱数を予測することが計算量的に困難となるような方法により生成された乱数は、暗号学的に安全な擬似乱数と呼ばれている。

【0017】この方法により生成された乱数列 $b_1$ 、 $b_2$ 、...、 $b_i$ のみから $b_{i+1}$ を求めることは、 $n$ を因数分解するのと同じだけの手間が必要であることが知られている。つまり、ある時点までに発生された乱数列のみからその時点以降に発生されるべき乱数を求めるための計算量は、 $n$ を因数分解するのに必要な計算量と同等であることが知られている。ただし、 $n$ を因数分解することを計算量的に困難にするためには $p$ 、 $q$ を数百ビット程度にする必要がある。このように、ある時点までに発生された乱数列のみからその時点以降に発生されるべき乱数を予測することが計算量的に困難となるような方法により生成された乱数は、暗号学的に安全な擬似乱数と呼ばれている。

【0018】しかし、乱数発生法として暗号学的に安全な擬似乱数発生方式を用いた場合には、前述のように $p$ 、 $q$ を数百ビット程度にする必要があり、その場合、式(3)の $x_{i+1} = x_i^2 \bmod n$ を計算するための計算量が大きく、高速に乱数を発生できないという問題があった。

【0019】

【課題を解決するための手段】上記課題を解決するために、本発明の乱数発生器は、データを保持する保持手段と、該保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する変換手段と、該変換手段による変換結果に基づき、前記保持手段に保持されるデータを更新する更新手段と、前記保持手段に保持されるデータの一部を、乱数系列として順次出力する出力手段とを具える。

【0020】また、本発明の他の態様によれば、データを保持する保持手段と、該保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する変換手段と、該変換手段による変換結果に基づき、前記保持手段に保持されるデータを更新する更新手段と、前記保持手段に保持されるデータの一部を、乱数系列として順次出力する出力手段と、前記パラメータとして出力系列から該系列を推定することが困難なパラメ

ータ系列を順次算出してパラメータを変更する算出手段とを具える。

【0016】方式Bの実現方法として、文献「アドバンセズ・イン・クリプトロジー」(“Advances in Cryptology”、1983年発行、PLENUM PRESS、61～78項)に示されているような方法が知られている。つまり、乱数列を $b_1$ 、 $b_2$ 、...とするとビット $b_i$ は、 $x_0$ を任意に与える初期値、 $p$ 、 $q$ を素数として、

ータ系列を順次算出してパラメータを変更する算出手段とを具える。

【0021】また、本発明の他の態様によれば、データを保持する第1の保持手段と、該第1の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第1の変換手段と、該第1の変換手段による変換結果に基づき、前記第1の保持手段に保持されるデータを更新する第1の更新手段と、前記第1の保持手段に保持されるデータの一部を、乱数系列として順次出力する第1の出力手段と、該第1の出力手段より出力される乱数系列に基づいて通信文を暗号化する暗号化手段とを送信装置に具え、データを保持する第2の保持手段と、該第2の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第2の変換手段と、該第2の変換手段による変換結果に基づき、前記第2の保持手段に保持されるデータを更新する第2の更新手段と、前記第2の保持手段に保持されるデータの一部を、乱数系列として順次出力する第2の出力手段と、該第2の出力手段より出力される乱数系列に基づいて暗号文を復号する復号手段とを受信装置に具える。

【0022】また、本発明の他の態様によれば、データを保持する第1の保持手段と、該第1の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第1の変換手段と、該第1の変換手段による変換結果に基づき、前記第1の保持手段に保持されるデータを更新する第1の更新手段と、前記第1の保持手段に保持されるデータの一部を、乱数系列として順次出力する第1の出力手段と、前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する第1の算出手段と、前記第1の出力手段より出力される乱数系列に基づいて通信文を暗号化する暗号化手段とを送信装置に具え、データを保持する第2の保持手段と、該第2の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第2の変換手段と、該第2の変換手段による変換結果に基づき、前記第2の保持手段に保持されるデータを更新する第2の更新手段と、前記第2の保持手段に保持されるデータの一部を、

乱数系列として順次出力する第 2 の出力手段と、前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する第 2 の算出手段と、前記第 2 の出力手段より出力される乱数系列に基づいて暗号文を復号する復号手段とを受信装置に具える。

【0023】

【作用】かかる本発明の乱数発生器においては、保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換手段により変換し、該変換手段による変換結果に基づき、前記保持手段に保持されるデータを更新手段が更新する。出力手段が前記保持手段に保持されるデータの一部を、乱数系列として順次出力する。

【0024】また、算出手段が前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する。

【0025】また、送信側で、データを保持する第 1 の保持部に保持されたデータを第 1 の変換部に入力し、所定のパラメータに基づいて入力データを変換し、該変換の結果に基づき、前記第 1 の保持部に保持されるデータを更新し、前記第 1 の保持部に保持されるデータの一部を、乱数系列として順次出力し、該出力される乱数系列に基づいて通信文を暗号化して暗号文を順次受信側に送信し、受信側で、データを保持する第 2 の保持部に保持されたデータを第 2 の変換部に入力し、所定のパラメータに基づいて入力データを変換し、該変換の結果に基づき、前記第 2 の保持部に保持されるデータを更新し、前記第 2 の保持部に保持されるデータの一部を、乱数系列として順次出力し、該出力される乱数系列に基づいて暗号文を復号する。

【0026】

【実施例】

（実施例 1）図 1 は、LFSR を用いた乱数発生器のブロック構成を示す図である。シフトレジスタ 11 及びシフトレジスタ 11 の各レジスタからの値を線形変換しシフトレジスタ 11 にフィードバックする線形変換回路 12 からなる。

【0027】本実施例による乱数発生の手順は以下の通りを行う（ただし手順 3、4、5 は同時に行われる）。

【0028】1. シフトレジスタ 11 の各レジスタに初期値を設定する。

【0029】2. 線形変換回路 12 は外部から与えられるパラメータに従って線形変換を決定する。

【0030】3. 各レジスタは与えられた値を右にシフトする。

【0031】4. 最右端のレジスタの値を乱数として出力する。

【0032】5. 各レジスタの値を 2. で決定された線形変換に従ってフィードバック変換し、最左端のレジ

スタの値とする。

【0033】6. 以下 3、4、5. を繰り返すが、式（2）による出力乱数列の解析が行えないようにするため、出力される乱数の数がその乱数列の解析に必要な乱数の数（今の場合シフトレジスタの段階の 2 倍）より大きくなる前に線形変換回路 12 に入力するパラメータを変更し、線形変換方式を変更する。

【0034】この手順において、手順 4. で出力される値の全て又は一部、或いは線形変換回路の出力の全て又は一部が本発明によって発生される乱数となる。線形変換回路に AND 回路を利用した場合の乱数発生器を図 2 に示す。図 2 において、まずシフトレジスタに初期値を設定する。AND 回路に接続されたレジスタの値は、前述のタップ列の値  $h_n$ 、 $h_{n-1}$ 、 $\dots$ 、 $h_2$ 、 $h_1$  を意味するので、レジスタの値を変更すれば線形変換方式を変更することになる。出力乱数系列の数がシフトレジスタの段数の 2 倍を越える前にパラメータの変更によってレジスタの値を変更すれば式（2）を解くことができず、乱数列を解析することができない。

【0035】また、手順 6. において、出力される乱数の数がその乱数列により決定される線形複雑度の 2 倍より大きくなった後に線形変換回路に入力するパラメータを変更し、線形変換方式を変更した場合でも、式（2）により解析されるのはその線形変換方式の場合だけであり、従来例のようにそれ以降の全ての乱数系列が解析されるのを防ぐことができるため、パラメータによって線形変換方式を変更した後は安全である。

【0036】（実施例 2）LFSR による乱数発生器では、出力乱数系列の解析に必要な乱数の数は LFSR の段数の 2 倍であるが、非線形フィードバックシフトレジスタを用いた場合には解析に必要な乱数の数を LFSR の場合以上に大きくすることが可能である。よって、式（2）による出力乱数列の解析に必要なビット数が多くなるので、非線形変換の方式を変えるパラメータの変更周期を大きくすることができるという利点がある。その非線形フィードバックシフトレジスタを用いた実施例を図 3 に示す。

【0037】図 3 は本発明による非線形フィードバックシフトレジスタを用いた場合の乱数列発生器を示すブロック図である。シフトレジスタ 11 及びシフトレジスタ 11 の各レジスタからの値を非線形変換しシフトレジスタ 11 にフィードバックする非線形変換回路 31 からなる。

【0038】本実施例による乱数発生の手順は以下の通りを行う（ただし手順 3、4、5. は同時に行われる）。

【0039】1. シフトレジスタ 11 の各レジスタに初期値を設定する。

【0040】2. 非線形変換回路 31 は外部から与えられるパラメータに従って非線形変換を決定する。

【0041】3. 各レジスタは与えられた値を右にシフトする。

【0042】4. 最右端のレジスタの値を乱数として出力する。

【0043】5. 各レジスタの値を2. で決定された非線形変換に従ってフィードバック変換し、最左端のレジスタの値とする。

【0044】6. 以下3. 4. 5. を繰り返すが、式(2)による出力乱数列の解析が行えないようにするため、出力される乱数の数とその乱数列の解析に必要な乱数の数より大きくなる前に非線形変換回路に入力するパラメータを変更し、非線形変換方式を変更する。

【0045】この手順において、手順4. で出力される値の全て又は一部、或いは非線形変換回路31の出力の全て又は一部が本実施例によって発生される乱数となる。具体的な非線形変換回路31の構成としては、公知の非線形関数の入出力の対応を記憶されたROM等によって実現できる。

【0046】(実施例3) 実施例1. 2. では、本発明をわかりやすく説明するため線形及び非線形フィードバックシフトレジスタを用いた例について述べたが、上記実施例の本質は与えられた初期値をもとに、定められた変換を施してフィードバックすることにより連鎖的に乱数を発生させる乱数発生方式において、該変換における変換方式を外部より与えるパラメータによって制御すること、特に変換方式を決定するのに必要なだけの乱数列を出力する前に該変換方式を制御するパラメータを変更し、該変換方式を変更すること、にある。このことから明かなように、乱数発生方式として線形及び非線形フィードバックシフトレジスタに限らず、種々の方式を用いることができるのは言うまでもない。

【0047】また、フィードバック変換における変換方式に関しても、外部から与えるパラメータによって制御する場合について述べてきたが、外部から与えるパラメータと内部で生成したパラメータを合成したパラメータによって制御することもできる。

【0048】(実施例4) 図4は、乱数を発生させる手順としてシフトレジスタを用いない場合を示している。

【0049】本実施例では、それぞれ同一のクロックで動作する $R_1 \sim R_n$ の $n$ 個のレジスタ、各レジスタからの出力と最終レジスタ( $R_n$ )からのフィードバック出力とで(非)線形変換を行い次のレジスタに出力する $S_1 \sim S_m$ の $m$ 個の(非)線形変換回路からなる。

【0050】本実施例による乱数発生の手順は以下の通りに行う(ただし手順3. 4. 5. は同時に行われる)。

【0051】1. 各レジスタにそれぞれ初期値を設定する。

【0052】2.  $S_1 \sim S_m$ の各(非)線形変換回路は外部から与えられるパラメータに従って(非)線形変換

を決定する。

【0053】3. 最右端のレジスタ( $R_n$ )の値を乱数として出力し、最左端のレジスタ( $R_1$ )の値とする。

【0054】4. 各レジスタは3. において保持していた値を出力すると同時に入力部にある値を保持する。

【0055】5. 各(非)線形変換回路は手前のレジスタから出力された値と $R_n$ からのフィードバック出力とを2. で決定された(非)線形変換によって変換し、後のレジスタに出力する。

【0056】6. 以下3. 4. 5. を繰り返すが、式(2)による出力乱数列の解析が行えないようにするため、出力される乱数の数とその乱数列の解析に必要な乱数の数より大きくなる前に(非)線形変換回路に入力するパラメータを変更し、(非)線形変換方式を変更する。

【0057】この手順において、 $R_n$ の出力の全て又は一部が本実施例によって発生される乱数となる。

【0058】また、上記手順において、各(非)線形変換回路は前述のROM等によって構成することができ、各(非)線形変換回路はそれぞれ異なる(非)線形変換を行っても良い。

【0059】(実施例5) 図5は擬似乱数発生器にDES(Data Encryption Standard)暗号回路を用いる場合の実施例を示している。最近差分解読法と呼ばれる有力な解読法が提案され、DES暗号の安全性に疑問が持たれるようになっており、その対策として鍵を頻繁に変更することが考えられる。DES暗号回路を用いる場合は、DES暗号の鍵を変えることが変換方式を変えることになる。

【0060】(実施例6) 以下の実施例によれば、前述の方式Aを用いた乱数発生器へ与えるパラメータを算出するために方式Bを用いたパラメータ算出回路を有し、このパラメータ算出回路より出力されるパラメータによって乱数発生器における変換方式を制御することによって、方式Aの利点である高速性と方式Bの利点である安全性の2つを実現する乱数列の発生を以下のようにして可能にしたものである。

【0061】方式Aによる乱数発生器に出力される乱数の数が、その乱数列の解析に必要な乱数の数より大きくなる前、或いは等しくなる近辺で前記タップ列の値を変更して乱数発生手段の変換の方式を変更させることにより、式(2)の方法による出力乱数列の解析が行えないようにし、出力乱数列の安全性を高めることができる。よって、そのタップ列の値をパラメータとして方式Bによって制御する。

【0062】この場合、方式Aを用いた乱数発生器によって出力される乱数の数とその乱数列の解析に必要な乱数の数より大きくなるまでに、方式Bによるパラメータの算出が行われれば良いため、方式Bの計算が高速に行えなくても全体として高速に乱数を生成することは可能

である。

【0063】また、式(2)の方法で解析を行うのに十分な数の乱数を出力した後に前記のタップ列の値を変更したとしても、解析できるのはそのタップ列の値の時だけである。しかもタップ列の値の制御は方式Bによって行われているので次のタップ列の値を予測することは困難であり、従来のようにそれ以降の全ての乱数系列が解析されるのを防ぐことができるため、タップ列の値を変更した後は安全である。

【0064】(実施例7) LFSRによる乱数発生器では、出力乱数系列の解析に必要な乱数の数はLFSRの段数の2倍であるが、非線形フィードバックシフトレジスタを用いた場合には解析に必要な乱数の数をLFSRの場合以上に大きくすることが可能である。よって、式(2)による出力乱数系列の解析に必要なビット数が多くなるので、非線形変換の方式を変えるためのパラメータの算出周期を大きくすることができるという利点がある。算出周期を大きくできることは、高速処理の困難な方式Bをパラメータ算出部に用いる場合に特に大きな利点となる。

【0065】その非線形フィードバックシフトレジスタを用いた実施例を図8に示す。図8は本発明による非線形フィードバックシフトレジスタを用いた場合の乱数発生器を示すブロック図である。方式Aに基づく乱数発生手段としてシフトレジスタ及びシフトレジスタの各レジスタからの値を非線形変換しシフトレジスタにフィードバックする非線形変換回路21を用い、方式Bに基づくパラメータ算出回路61を用いて構成される。非線形変換方式はパラメータ算出回路61からの出力により制御される。

【0066】本実施例による乱数発生手順は以下の通りに行う(ただし手順4. 5. 6. は同時に行われる)。

【0067】1. シフトレジスタの各レジスタ及びパラメータ算出回路に初期値を設定する。

【0068】2. パラメータ算出回路は与えられた初期値から第一のパラメータを算出し、非線形変換回路21に出力する。

【0069】3. 非線形変換回路21は、2. により与えられるパラメータに従って非線形変換を決定する。

【0070】4. 各レジスタは与えられた値を右にシフトする。

【0071】5. 最右端のレジスタの値を乱数として出力する。

【0072】6. 各レジスタの値を3. で決定された非線形変換に従ってフィードバック変換し、最左端のレジスタの値とする。

【0073】7. 以下4. 5. 6. を繰り返すが、式(2)による出力乱数系列の解析が行えないようにするため、出力される乱数の数がその乱数系列の解析に必要な乱数の数より大きくなる前にパラメータ算出回路は次のパ

ラメータを算出し、非線形変換回路21に出力して非線形変換方式を変更する。

【0074】この手順において、手順5. で出力される値の全て又は一部、或いは非線形変換回路の出力の全て又は一部が本発明によって発生される乱数となる。具体的な非線形変換回路21の構成としては、公知の非線形関数の入出力の対応を記憶させたROM等によって実現できる。

【0075】(実施例8) 実施例6. 7では、本発明をわかりやすく説明するため乱数発生手段として線形及び非線形フィードバックシフトレジスタを用いた例について述べたが、本発明の本質は方式Aを用いた乱数発生手段の変換方式を方式Bを用いたパラメータ算出手段から出力されるパラメータによって制御することにある。特に乱数発生手段の変換方式を決定するのに必要なだけの乱数系列を出力する前に該変換方式をパラメータ算出手段からの出力により変更することにある。このことから明らかなように、乱数発生手段として線形及び非線形フィードバックシフトレジスタに限らず、種々の方式を用いることができるのは言うまでもない。

【0076】また、方式Bとして用いることのできる暗号的に安全な擬似乱数発生法には、式(3)の他に文献「暗号と情報セキュリティ」(辻井、笠原著、1990年発行、株式会社昭晃社、86頁)に示されているように、RSA暗号、離散対数、逆数暗号を用いたものが知られており、これらも本発明のパラメータ算出手段のアルゴリズムに用いることができる。

【0077】また、図2のように暗号的に安全な擬似乱数発生法と内容が秘密にされたROMをフィードバック的に用いる方法を組み合わせることによっても方式Bに基づくパラメータ発生手段は構成できる。

【0078】また、内容が秘密にされたROMをフィードバック的に用いる方法だけでも、それまでにそのROMから発生した値からROM内部の残りの値を知ることとはできないため、方式Bに基づくパラメータ発生手段は構成できる。

【0079】さらに、乱数発生手段の変換方式の制御に関してもパラメータ算出回路により生成されたパラメータによってのみ制御する場合について述べてきたが、乱数発生手段の内部のパラメータとパラメータ算出回路で算出したパラメータとを合成したパラメータによって制御することもできる。

【0080】(実施例9) 図9は、乱数を発生させる手順としてシフトレジスタを用いない場合を示している。

【0081】本実施例では、方式Aに基づく乱数発生手段としてそれぞれ同一のクロックで動作する $R_1 \sim R_s$ の $s$ 個のレジスタ及び各レジスタからの出力と最終レジスタ( $R_s$ )からのフィードバック出力とで(非)線形変換を行い次のレジスタに出力する $T_1 \sim T_m$ の $m$ 個の(非)線形変換回路を用い、方式Bに基づくパラメータ

算出回路61を用いて構成される。各（非）線形変換方式はパラメータ算出回路61からの出力により制御される。

【0082】本実施例による乱数発生の手順は以下の通りを行う（ただし手順4. 5. 6. は同時に行われる）。

【0083】1. 各レジスタ及びパラメータ算出回路61にそれぞれ初期値を設定する。

【0084】2. パラメータ算出回路61は与えられた初期値から第一のパラメータを算出し、各（非）線形変換回路に出力する。

【0085】3.  $T_1 \sim T_m$  の各（非）線形変換回路は2. により与えられるパラメータに従ってそれぞれの（非）線形変換を決定する。

【0086】4. 最右端のレジスタ（ $R_S$ ）の値を乱数として出力し、最左端のレジスタ（ $R_1$ ）の値とする。

【0087】5. 各レジスタは4. において保持していた値を出力すると同時に入力部にある値を保持する。

【0088】6. 各（非）線形変換回路は手前のレジスタから出力された値と $R_S$ からのフィードバック出力とを3. で決定された（非）線形変換によって変換し、後のレジスタに出力する。

【0089】7. 以下4. 5. 6. を繰り返すが、式（2）による出力乱数列の解析が行えないようにするため、出力される乱数の数がその乱数列の解析に必要な乱数の数より大きくなる前にパラメータ算出回路は次のパラメータを算出し、各（非）線形変換回路に出力してそれぞれの（非）線形変換方式を変更する。

【0090】この手順において、 $R_S$ の出力の全て又は一部が本発明によって発生される乱数となる。

【0091】また、上記手順において、各（非）線形変換回路は前述のROM等によって構成することができ、各（非）線形変換回路はそれぞれ異なる（非）線形変換を行っても良い。

【0092】（実施例10）図10は本発明において乱数発生手段にDES（Data Encryption Standard）暗号回路51を用いる場合の実施例を示している。最近差分解読法と呼ばれる有力な解読法が提案され、DES暗号の安全性に疑問が持たれるようになっており、その対策として鍵を頻繁に変更することが考えられる。DES暗号装置51を用いる場合は、DES暗号の鍵を変えることが変換方式を変えることになる。

【0093】（実施例11）これまでに述べたように、上記の乱数発生器によって生成された乱数は解析に対して強いので、この乱数を暗号化方式に用いることにより解析に対して強く安全性の高い暗号通信が実現できる。以下、通信文と乱数との間でビット毎に排他的論理和をとる暗号化方式（ストリーム暗号）による暗号通信ネットワークにおいて、乱数発生器を用いた暗号通信の実施

例を示す。

【0094】図11はネットワークの加入者間で固有かつ秘密の暗号鍵を共有している共通鍵暗号通信ネットワークを示し、A、B、C、…、Nはそのネットワークの加入者、 $K_{AB}$ 、 $K_{AC}$ 、…はそれぞれ加入者A-B間で共有している暗号鍵、加入者A-C間で共有している暗号鍵、…を示している。

【0095】図12は本発明による乱数発生回路とパラメータ算出回路からなる乱数発生器121を用いた場合の暗号装置及び復号装置を含む通信装置122の構成を示したブロック図である。

【0096】図13は図11、図12で示された暗号通信システムにおけるA、B間の秘匿通信の様子を示している。

【0097】加入者Aから加入者Bへの暗号通信は以下の手順で行う。

【0098】1. 通信の送信者Aは、送信先Bと共有している秘密の鍵 $K_{AB}$ の全て又は一部を乱数発生回路及びパラメータ算出回路の初期値として設定し、乱数系列 $k_i$ を発生させる。

【0099】2. Aは発生した乱数系列 $k_i$ と通信文 $m_i$ をビット毎に排他的論理和をとり、暗号文

【0100】

【外3】

$$c_i = m_i \oplus k_i$$

を計算し、その暗号文をBに送信する。

【0101】3. 通信の受信者Bは、送信元Aと共有している秘密の鍵 $K_{AB}$ の全て又は一部を乱数発生回路及びパラメータ算出回路の初期値として設定し、送信者が発生したのと同じ乱数系列 $k_i$ を発生させる。

【0102】4. Bは発生した乱数系列 $k_i$ と受信暗号文 $c_i$ をビット毎に排他的論理和をとり、通信文

【0103】

【外4】

$$m_i = c_i \oplus k_i$$

を復元する。

【0104】この手順に従えば、正規の送信先Bだけがその秘密の鍵 $K_{AB}$ を知っているのを受け取った暗号文を本来の通信文に復号でき、それ以外の加入者（C～N）はその暗号文をする際に用いられた秘密の鍵を知らないなのでその内容を知ることができない。このことにより秘匿通信が実現される。また、図11のようにあらかじめ暗号鍵が配布されているのではなく、暗号通信を行うに先立って送・受信者間で暗号鍵を共有する必要がある形態のネットワークにおいても、公知の手法で鍵共有を行えば同じ手順で暗号通信を実現することができる。

【0105】（実施例12）実施例11に示した暗号通信ネットワークでは通信文の送信者と受信者の間で固有



かつ秘密の鍵を共有しているので、暗号文を受け取り、意味をなす通信文に復号できるということは、通信文がその鍵のもう一人の所有者から送信されたことを受信者に保証している。そのため、実施例 11 に示した秘匿通信システムでは、通信の発信者及び着信者の認証も行うことができる。

【0106】（実施例 13）実施例 11、12 のようにあらかじめ暗号鍵が配布されているのではなく、暗号通信を行うに先立って送・受信者間で暗号鍵を共有する必要がある形態のネットワークにおいて、盗聴の可能性のある通信路を介した場合でも安全に暗号鍵を共有できる方式として Diffie-Hellman の方式（W. Diffie and M. E. Hellman “New Directions in cryptography”, IEEE, IT, vol. 1, T-22, No. 6, 1976）がよく知られている。その際に用いる乱数として本発明により発生した乱数を用いることができる。

【0107】その場合に用いる乱数は、送信者と着信者で同じものを持つ必要はないため、乱数発生手段及びパラメータ発生手段に設定する初期値は任意の値を用いれば良い。

【0108】

【発明の効果】以上説明したように、本発明によれば、一定数の出力系列から解析可能な方式（方式 A）により出力される乱数の数が、その解析に必要な数より大きくなる前、或いは等しくなる近辺で、方式 A のパラメータを変更するので、方式 A の解析に必要な数の出力を集めることが困難になり、発生する乱数の安全性が高められるという効果がある。

【0109】また、方式 A のパラメータを、出力系列から解析困難な方式（方式 B）により出力される乱数に基づいて変更することにより、方式 A の安全性が一層高められるという効果がある。

【0110】この場合、方式 A から出力される出力の数が方式 A の解析に必要な数より大きくなるまでに、方式 B による乱数の出力が行われれば良いため、方式 B の乱数発生は高速に行えなくてもよい。しかし、最終出力は方式 A からの出力であるので、高速に乱数を発生することが可能である。

【0111】また、この乱数系列を暗号通信に用いれば、高速かつ安全性の高い暗号通信が実現されるという

効果がある。

【図面の簡単な説明】

【図 1】LFSR を用いた乱数発生器のブロック構成を示す図である。

【図 2】LFSR を用いた乱数発生器の詳細なブロック構成を示す図である。

【図 3】非線形フィードバックレジスタを用いた乱数発生器のブロック構成を示す図である。

【図 4】複数のレジスタを用いた乱数発生器のブロック構成を示す図である。

【図 5】DES 暗号装置を用いた乱数発生器のブロック構成を示す図である。

【図 6】LFSR を用いた乱数発生器のブロック構成を示す図である。

【図 7】LFSR を用いた乱数発生器のブロック構成を示す図である。

【図 8】非線形フィードバックレジスタを用いた乱数発生器のブロック構成を示す図である。

【図 9】複数のレジスタを用いた乱数発生器のブロック構成を示す図である。

【図 10】DES 暗号装置を用いた乱数発生器のブロック構成を示す図である。

【図 11】共通鍵暗号通信ネットワークを説明する図である。

【図 12】暗号装置及び復号装置を含む通信装置の構成を示すブロック図である。

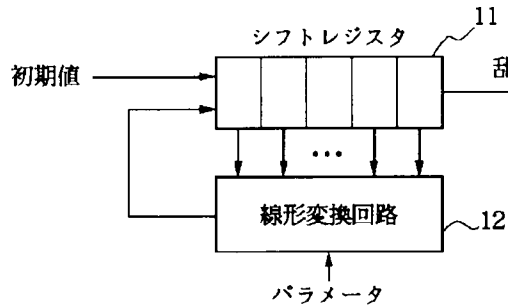
【図 13】秘匿通信を行う通信システムを説明する図である。

【図 14】LFSR を用いた従来の乱数発生器のブロック構成を示す図である。

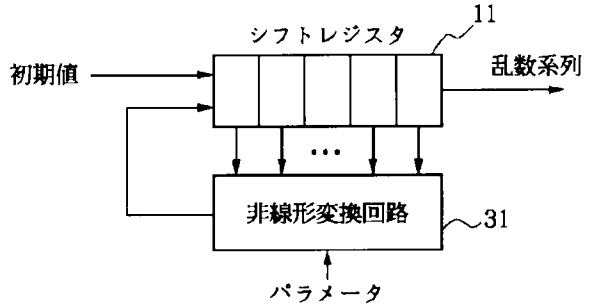
【符号の説明】

- 11 シフトレジスタ
- 12 線形変換回路
- 21 レジスタ
- 31 非線形変換回路
- 51 DES 暗号回路
- 61 パラメータ算出回路
- 71 ROM
- 72 バッファ
- 73 自乗剰余算回路
- 121 乱数発生器
- 122 通信装置

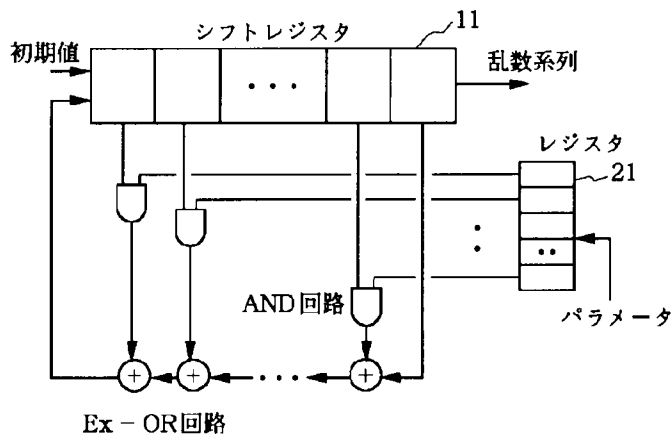
【図1】



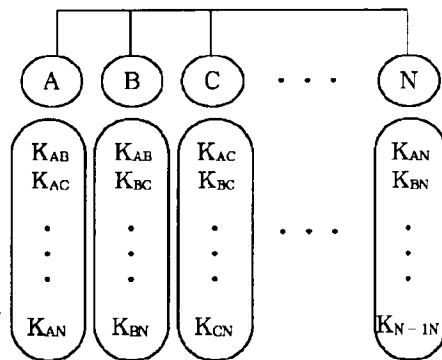
【図3】



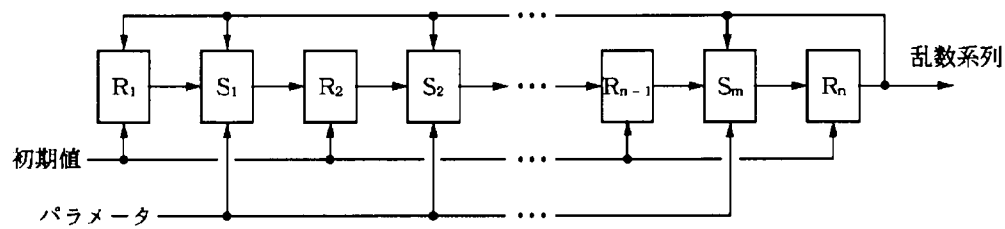
【図2】



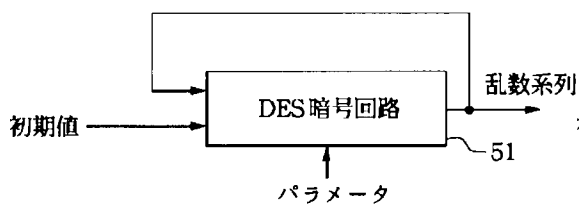
【図11】



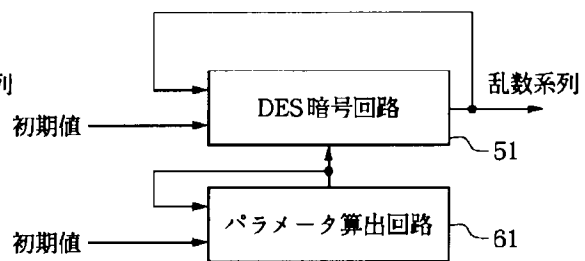
【図4】



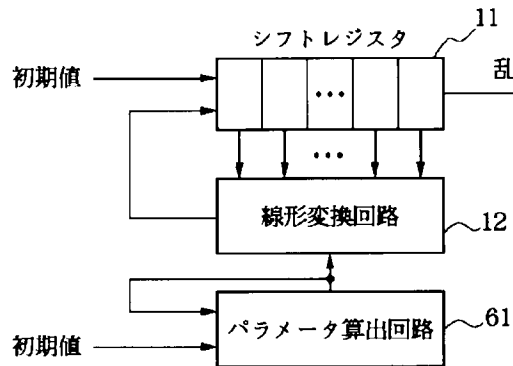
【図5】



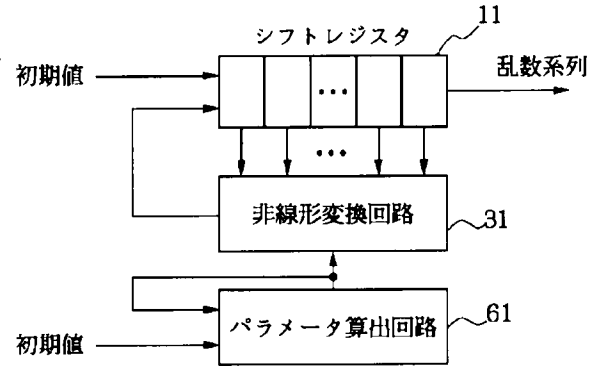
【図10】



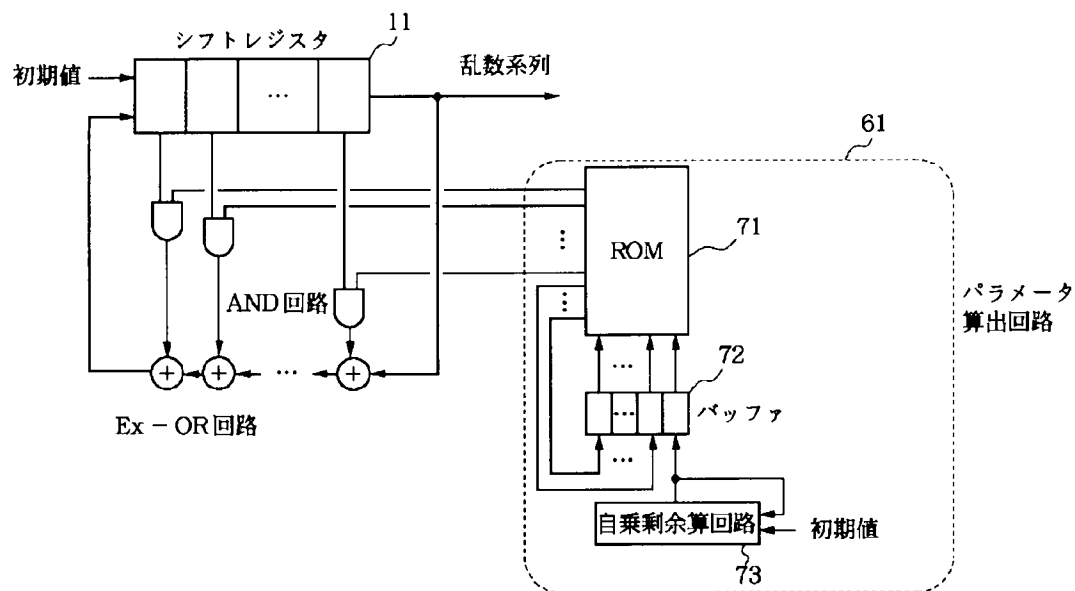
【図6】



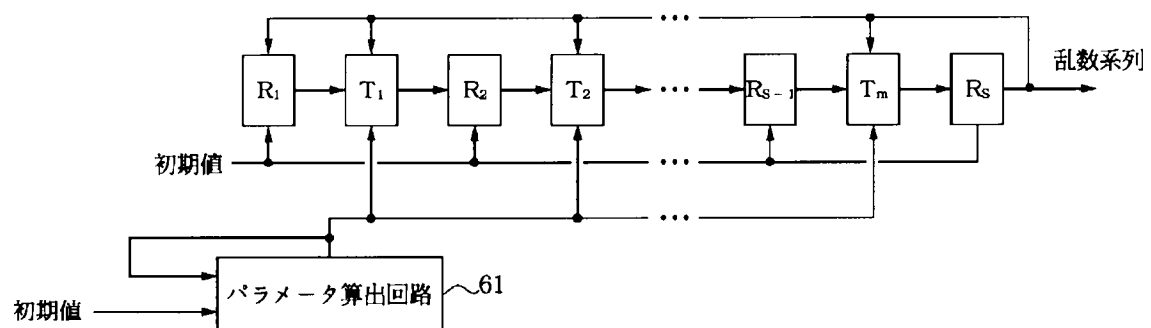
【図8】



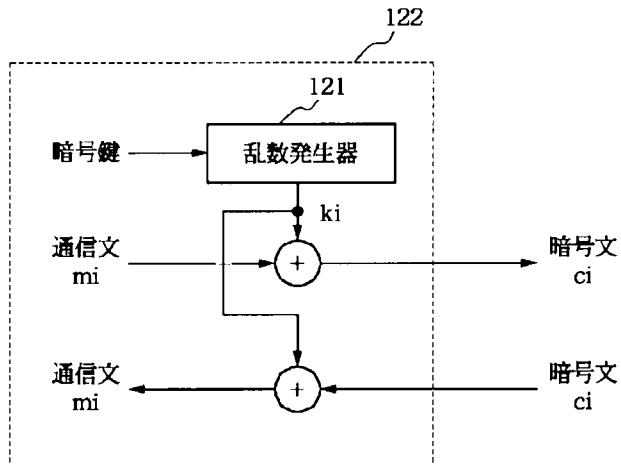
【図7】



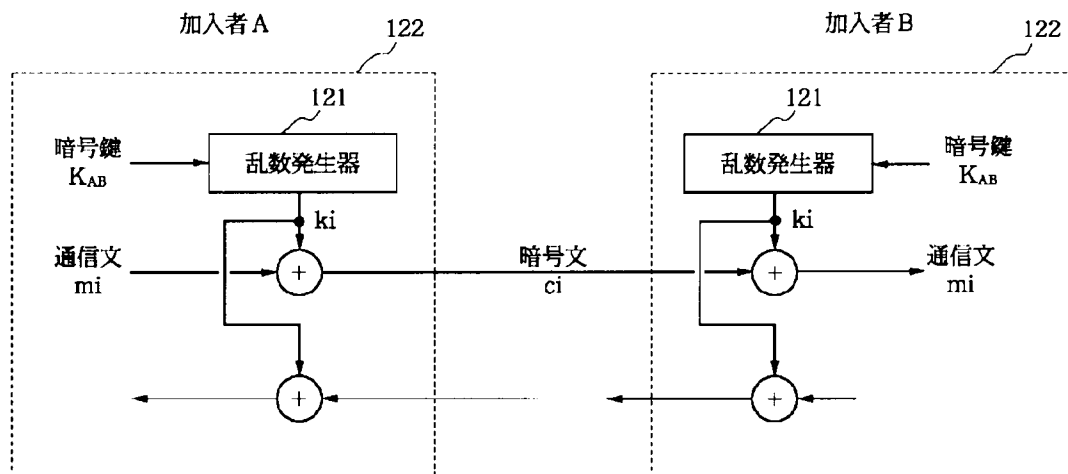
【図9】



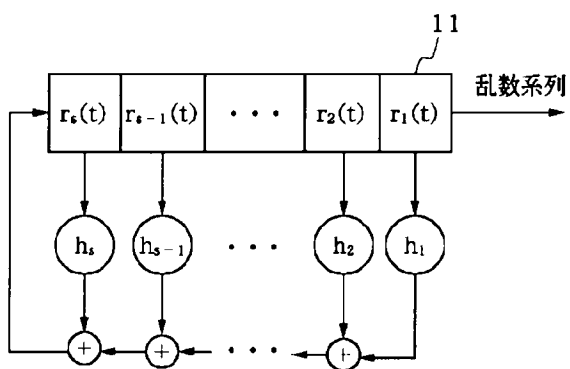
【図 12】



【図 13】



【図 14】



# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-036672

(43)Date of publication of application : 07.02.1995

---

(51)Int.Cl. G06F 7/58  
G09C 1/00  
H04L 9/22

---

(21)Application number : 05-179232 (71)Applicant : CANON INC  
(22)Date of filing : 20.07.1993 (72)Inventor : YAMAMOTO TAKAHISA  
IWAMURA KEIICHI

---

**(54) RANDOM-NUMBER GENERATOR COMMUNICATION SYSTEM USING THE  
SAME AND METHOD THEREFOR**

(57)Abstract:

PURPOSE: To generate a safe random number sequence at a high speed.

CONSTITUTION: This generator is provided with a shift register 1 bonding data a linear conversion circuit 12 inputting the data held in the shift register 11 and converting an inputted data value based on a prescribed parameter an update means updating the data held in the shift register 11 based on the conversion result by the linear conversion circuit 12 and an output means successively outputting the partial data held in the shift register 11 as a random number sequence.

---

## CLAIMS

---

[Claim(s)]

[Claim 1] Holding mechanism holding data and a conversion method which inputs data held at this holding mechanism and changes an input data value based on a predetermined parameter A random number generator having an update means which updates data held at said holding mechanism and an output means which outputs some data held at said holding mechanism one by one as a random number series based on a conversion result by this conversion method and changing said parameter with a predetermined cycle.

[Claim 2] A random number generator comprising:  
Holding mechanism holding data.

A conversion method which inputs data held at this holding mechanism and changes an input data value based on a predetermined parameter.

An update means which updates data held at said holding mechanism based on a conversion result by this conversion method.

An output means which outputs some data held at said holding mechanism one by one as a random number series and a calculating means which presuming this series from a power range system sequence as said parameter computes a difficult parameter series one by one and changes a parameter.

[Claim 3] The 1st holding mechanism holding data and the 1st conversion method that inputs data held at this 1st holding mechanism and changes an input data value based on a predetermined parameter. The 1st update means that updates data held at said 1st holding mechanism based on a conversion result by this 1st conversion method. The 1st output means that outputs some data held at said 1st holding mechanism one by one as a random number series. The 2nd holding mechanism that equips a sending set with an encoding means which enciphers correspondence based on a random number series outputted from this 1st output means and holds data. The 2nd conversion method that inputs data held at this 2nd holding mechanism and changes an input data value based on a predetermined parameter. The 2nd update means that updates data held at said 2nd holding mechanism based on a conversion result by this 2nd conversion method. A communications system equipping a receiving set with the 2nd output means that outputs some data held at said 2nd holding mechanism one by one as a random number series and a decoding means which decodes a cryptogram based on a random number series outputted from this 2nd output means.

[Claim 4] The 1st holding mechanism holding data and the 1st conversion method that inputs data held at this 1st holding mechanism and changes an input data value based on a predetermined parameter. The 1st update means that updates data held at said 1st holding mechanism based on a conversion result by this 1st conversion method. The 1st output means that outputs some data held at said 1st holding mechanism one by one as a random number series. The 1st calculating means that presuming this series from a power range system sequence as said parameter computes a difficult parameter series one by one and changes a parameter. The 2nd holding mechanism that equips a sending set with an encoding means which enciphers correspondence based on a random number series outputted from said 1st output means and holds data. The 2nd conversion method that inputs data held at this 2nd holding mechanism and changes an input data value based on a predetermined parameter. The 2nd update means that updates data held at said 2nd holding mechanism based on a conversion result by this 2nd conversion method and the 2nd output means that outputs some data held at said 2nd holding mechanism one by one as a random number series. The 2nd calculating means that presuming this series from

a power range system sequence as said parameter computes a difficult parameter series one by one and changes a parameter. A communications system equipping a receiving set with a decoding means which decodes a cryptogram based on a random number series outputted from said 2nd output means.

[Claim 5] Data held at the transmitting side at the 1st attaching part holding data is inputted into the 1st converter. Based on a predetermined parameter change input data and based on a result of this conversion, one by one, update data held at said 1st attaching part, output some data held at said 1st attaching part one by one as a random number series, encipher correspondence based on a random number series, this outputted, transmit to a receiver, and a cryptogram by a receiver. Data held at the 2nd attaching part holding data is inputted into the 2nd converter. Based on a predetermined parameter change input data and based on a result of this conversion, A correspondence procedure updating data held at said 2nd attaching part, outputting some data held at said 2nd attaching part one by one as a random number series, and decoding a cryptogram based on a random number series, this outputted.

[Claim 6] Data held at the transmitting side at the 1st attaching part holding data is inputted into the 1st converter. Based on a predetermined parameter change input data and based on a result of this conversion, update data held at said 1st attaching part, presuming this series from a power range system sequence as said parameter computes a difficult parameter series one by one, and a parameter is changed. At the time of order, transmit to a receiver, and a cryptogram which outputs some data held at said 1st attaching part one by one as a random number series, and enciphers correspondence based on a random number series, this outputted by a receiver. Data held at the 2nd attaching part holding data is inputted into the 2nd converter. Based on a predetermined parameter change input data and based on a result of this conversion, update data held at said 2nd attaching part, and presuming this series from a power range system sequence as said parameter computes a difficult parameter series one by one, and it updates a parameter. A correspondence procedure outputting some data held at said 2nd attaching part one by one as a random number series, and decoding a cryptogram based on a random number series, this outputted.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Industrial Application] Especially this invention relates to secrecy of the data in the encryption communication field, attestation of an addresser and an action addressee, sharing of an encryption key, a zero knowledge proof protocol, etc. with regards to a cipher system. It is related with the simulation using random numbers, such as a Monte Carlo simulation.

[0002]

[Description of the Prior Art] Conventionally as one of the random variate generation methods the thing using the linear feedback shift register (LFSR) which generates a maximum length periodic system sequence (M sequence) is known as shown in the 69-72nd page of literature "present age code theory" (Ikano Akira Koyama the Showa 61 issue Institute of Electronics Information and Communication Engineers).

[0003] it is indicated in drawing 14 as a LFSR method -- as -- shift register  $R(t) = (r_s(t), \dots, r_2(t), r_1(t))$  and a tap (bay line) sequence  $(h_{s-1}, \dots, h_2, h_1)$  and It is the method of generating a pseudo random number system by consisting of  $h_{s-1}, \dots, h_2$  and  $h_1$  and performing the following operations simultaneously to each every time (stop).

[0004] (a) Output bit  $r_1(t)$  of a rightmost register as a pseudo random number system.

[0005]  $k_t = r_1(t)$

(b)  $r_s(t), r_{s-1}(t), \dots$  and  $r_2(t)$  are shifted to the right.

[0006]  $r_i(t+1) = r_{i+1}(t)$  ( $i = 1, 2, \dots, s-1$ )

(c) Calculate bit  $r_s(t+1)$  of the register of a high order end as follows by the contents and the tap sequence of a register.

[0007]

[External Character 1]

When it collects above the pseudorandom-numbers generation algorithm of a LFSR method uses the procession H of an s line s sequence and is  $R(t+1) = H - R(t) \bmod 2$  (1).

Jam [0008]

[External Character 2]

It can express.

[0009] If the tap sequence of LFSR of this s stage is chosen well the bit series of the pseudorandom numbers of maximum cycle  $2^s - 1$  can be generated and the series at that time will turn into the above-mentioned maximum length periodic system sequence.

[0010] However in the random variate generation method using this LFSR the tap sequence  $(h_s, h_{s-1}, \dots, h_2, h_1)$  of s stage can be determined by the following methods from 2-s bit output pseudo-random number sequence using the linearity of LFSR.

[0011] The pseudo random number systems outputted are  $k_1, k_2$  and  $\dots$ . Supposing it is  $k_{2s}$ . At a certain time the contents  $R(t)$  of the register of  $t$  ( $t = 1, 2, \dots, s+1$ ).  $R(1) = (k_s, k_{s-1}, \dots, k_1)^T$  (2)  $= (k_{s+1}, \dots, k_2)^T$  -- It can express  $R(s+1) = (k_{2s}, k_{2s-1}, \dots, k_{s+1})^T$  ( $^T$  shows transposition).

At this time they are the processions X and Y  $X = (R(1), R(2), \dots, R(s))$

$Y = (R(2), R(3), \dots, R(s+1))$

Since the relation of  $Y = H - X$  will be materialized from a formula (1) if it carries out it is  $H = Y - X^{-1}$  (2).



It is alike  $H$  is called for more and a tap sequence is determined.

[0012] That is although the cycle of a random number is  $2^s - 1$  it opts for the composition of LFSR by a bit for 2 of them  $s$ . In this case since all the random number sequences generated henceforth at that time were known there was a fault that it was unsuitable in respect of safety using an output random number sequence as a random number for codes.

[0013] If a nonlinear feedback shift register is used it is known that the number of the random numbers which are needed for the analysis of an output random number series can be enlarged. however BARE comp Massey's algorithm (E. — R. Berlekamp "Algebraic coding theory".) McGraw-Hill Book Company and LFSR of the minimum number of stages which can generate the series by 1968 could be calculated and the random number generation method using a nonlinear feedback shift register may also have been analyzed by the method of the formula (2).

[0014] As mentioned above if the output random number of a certain time can be got the random number generation method which can predict easily all the random number sequences outputted after it will be called the method A for convenience. Although the method A is not safe in cryptography as mentioned above since composition is easy it has the feature that high speed processing is possible.

[0015] Unlike the method A the random variate generation method with which it becomes very difficult to predict the random number which should be generated henceforth at that time only from the random number sequence generated by a certain point in time is shown below and it will be called the method B for convenience.

[0016] As a realization method of the method B the method as shown in literature "ADOBANSEZU yne cryptology" ("Advances in Cryptology" the 1983 issue PLENUM PRESS 61 – 78 paragraph) is known. That is if a random number sequence is made into  $b_1, b_2$  and ... bit  $b_i$  will make a prime number the initial value and  $p$  which give  $x_0$  arbitrarily and  $q$  and it is  $x_{i+1} = x_i^2 \bmod n$  ( $i = 0, 1, 2, \dots$ ) (3).

$b_i = \text{lsb}(x_i)$  ( $i = 0, 1, 2, \dots$ )

Be alike is given (however  $n = p - q$  and  $\text{lsb}$  express a least significant bit).

[0017] Random number sequence  $b_1$  generated by this method  $b_2, \dots$  It is known that only the time and effort which is the same as factoring  $n$  is required for asking for  $b_i$  to  $b_{i+1}$ . That is it is known that the computational complexity for asking for the random number which should be generated henceforth at that time only from the random number sequence generated by a certain point in time is equivalent to computational complexity required to factor  $n$ . However in order to make it difficult to factor  $n$  in computational complexity  $p$  and  $q$  need to be about hundreds of bits. Thus the random number generated by the way it becomes difficult in computational complexity to predict the random number which should be generated henceforth at that time only from the random number sequence generated by a certain point in time is called pseudorandom numbers safe in cryptography.

[0018] However when a pseudorandom-numbers generating system safe in

cryptography is used as a random variate generation method.  $p$  and  $q$  needed to be about hundreds of bits as mentioned above and there was a problem that the computational complexity for calculating  $x_{i+1} = x_i^2 \bmod n$  of a formula (3) in that case was large and a random number could not be generated at high speed.

[0019]

[Means for Solving the Problem] In order to solve an aforementioned problem a random number generator of this invention is provided with the following.

Holding mechanism holding data.

A conversion method which inputs data held at this holding mechanism and changes an input data value based on a predetermined parameter.

An update means which updates data held at said holding mechanism based on a conversion result by this conversion method.

An output means which outputs some data held at said holding mechanism one by one as a random number series.

[0020] Holding mechanism which holds data according to other modes of this invention and a conversion method which inputs data held at this holding mechanism and changes an input data value based on a predetermined parameter. An update means which updates data held at said holding mechanism based on a conversion result by this conversion method. It has an output means which outputs some data held at said holding mechanism one by one as a random number series and a calculating means which presuming this series from a power range system sequence as said parameter computes a difficult parameter series one by one and changes a parameter.

[0021] The 1st holding mechanism that holds data according to other modes of this invention. The 1st conversion method that inputs data held at this 1st holding mechanism and changes an input data value based on a predetermined parameter. The 1st update means that updates data held at said 1st holding mechanism based on a conversion result by this 1st conversion method. The 1st output means that outputs some data held at said 1st holding mechanism one by one as a random number series. The 2nd holding mechanism that equips a sending set with an encoding means which enciphers correspondence based on a random number series outputted from this 1st output means and holds data. The 2nd conversion method that inputs data held at this 2nd holding mechanism and changes an input data value based on a predetermined parameter. The 2nd update means that updates data held at said 2nd holding mechanism based on a conversion result by this 2nd conversion method. A receiving set is equipped with the 2nd output means that outputs some data held at said 2nd holding mechanism one by one as a random number series and a decoding means which decodes a cryptogram based on a random number series outputted from this 2nd output means.

[0022] The 1st holding mechanism that holds data according to other modes of this invention. The 1st conversion method that inputs data held at this 1st holding

mechanism and changes an input data value based on a predetermined parameter. The 1st update means that updates data held at said 1st holding mechanism based on a conversion result by this 1st conversion method. The 1st output means that outputs some data held at said 1st holding mechanism one by one as a random number series. The 1st calculating means that presuming this series from a power range system sequence as said parameter computes a difficult parameter series one by one and changes a parameter. The 2nd holding mechanism that equips a sending set with an encoding means which enciphers correspondence based on a random number series outputted from said 1st output means and holds data. The 2nd conversion method that inputs data held at this 2nd holding mechanism and changes an input data value based on a predetermined parameter. The 2nd update means that updates data held at said 2nd holding mechanism based on a conversion result by this 2nd conversion method and the 2nd output means that outputs some data held at said 2nd holding mechanism one by one as a random number series. Presuming this series from a power range system sequence as said parameter equips a receiving set with the 2nd calculating means that computes a difficult parameter series one by one and changes a parameter and a decoding means which decodes a cryptogram based on a random number series outputted from said 2nd output means.

[0023]

[Function] In the random number generator of this invention, the data held at holding mechanism is inputted, an input data value is changed by a conversion method based on a predetermined parameter, and an update means updates the data held at said holding mechanism based on the conversion result by this conversion method. An output means outputs some data held at said holding mechanism one by one as a random number series.

[0024] It computes a difficult parameter series that a calculating means presumes this series from a power range system sequence as said parameter one by one and a parameter is changed.

[0025] The data held at the transmitting side at the 1st attaching part holding data is inputted into the 1st converter. Based on a predetermined parameter, change input data and based on the result of this conversion, one by one update the data held at said 1st attaching part, output some data held at said 1st attaching part one by one as a random number series, encipher correspondence based on the random number series, this outputted, transmit to a receiver, and a cryptogram by a receiver. The data held at the 2nd attaching part holding data is inputted into the 2nd converter. Input data is changed based on a predetermined parameter, the data held at said 2nd attaching part is updated based on the result of this conversion, some data held at said 2nd attaching part is outputted one by one as a random number series, and a cryptogram is decoded based on the random number series, this outputted.

[0026]

[Example]

(Example 1) Drawing 1 is a figure showing the block configuration of the random number generator which used LFSR. It consists of the linear transform circuit 12 which carries out linear transform of the value from each register of the shift register 11 and the shift register 11 and is fed back to the shift register 11.

[0027]The procedure of the random number generation by this example is followed for the following to pass (however Procedure 3.4.5 is performed simultaneously).

[0028]1. Set an initial value as each register of the shift register 11.

[0029]2. The linear transform circuit 12 opts for linear transform according to the parameter given from the outside.

[0030]3. Each register shifts the given value to the right.

[0031]4. Output the value of a rightmost register as a random number.

[0032]5. Carry out feedback transformation of the value of each register according to the linear transform for which it opted by 2. and consider it as the value of the register of a high order end.

[0033]6. Although 3.4.5. is repeated below In order to be unable to analyze the output random number sequence by a formula (2) before becoming larger than the number of the random numbers which the number of the random numbers outputted needs for the analysis of the random number sequence (in the case of now twice of the stage of a shift register) the parameter inputted into the linear transform circuit 12 is changed and a linear transform method is changed.

[0034]In this procedure all or a part of output of a linear transform circuit serves as all the values outputted by procedure 4. or a random number generated by this invention in part. The random number generator at the time of using an AND circuit for a linear transform circuit is shown in drawing 2. In drawing 2 an initial value is first set as a shift register. Since the value of the register connected to the AND circuit means value  $h_n$  of the above-mentioned tap sequence  $h_{n-1} \dots h_2$  and  $h_1$  if the value of a register is changed a linear transform method will be changed. If the value of a register is changed by change of a parameter before the number of output random number series exceeds the twice of the number of stages of a shift register a formula (2) cannot be solved and a random number sequence cannot be analyzed.

[0035]The parameter inputted into a linear transform circuit after the number of the random numbers outputted becomes larger [ the linearity complexity determined by the random number sequence ] than twice in procedure 6. is changed Even when a linear transform method is changed only in the case of the linear transform method it is analyzed by the formula (2) and since it can prevent analyzing all the random number series after it like a conventional example it is safe after changing a linear transform method with a parameter.

[0036](Example 2) Although the number of random numbers required for the analysis of an output random number series is twice the number of stages of LFSR in the random number generator by LFSR when a nonlinear feedback shift register is used it is possible to make the number of random numbers required for analysis large beyond

[ of LFSR ] a case. Therefore since the number of bits required for the analysis of the output random number sequence by a formula (2) increases there is an advantage that the change period of the parameter which changes the method of nonlinear transformation can be enlarged. The example using the nonlinear feedback shift register is shown in drawing 3.

[0037] Drawing 3 is a block diagram showing the random number sequence generator at the time of using the nonlinear feedback shift register by this invention. It consists of the nonlinear transformation circuit 31 which carries out nonlinear transformation of the value from each register of the shift register 11 and the shift register 11 and is fed back to the shift register 11.

[0038] The procedure of the random number generation by this example is followed for the following to pass (however procedure 3.4.5. is performed simultaneously).

[0039] 1. Set an initial value as each register of the shift register 11.

[0040] 2. The nonlinear transformation circuit 31 opts for nonlinear transformation according to the parameter given from the outside.

[0041] 3. Each register shifts the given value to the right.

[0042] 4. Output the value of a rightmost register as a random number.

[0043] 5. Carry out feedback transformation of the value of each register according to the nonlinear transformation for which it opted by 2. and consider it as the value of the register of a high order end.

[0044] 6. Although 3.4.5. is repeated below in order to be unable to analyze the output random number sequence by a formula (2) change the parameter inputted into a nonlinear transformation circuit before becoming larger than the number of the random numbers which the number of the random numbers outputted needs for the analysis of the random number sequence and change a nonlinear transformation method.

[0045] In this procedure all or a part of output of the nonlinear transformation circuit 31 serves as all the values outputted by procedure 4. or a random number generated by this example in part. It is realizable by ROM etc. which had correspondence of input and output of a publicly known nonlinear function memorized as composition of the concrete nonlinear transformation circuit 31.

[0046] (Example 3) By example 1.2. in order to explain this invention plainly described the example using linearity and a nonlinear feedback shift register but. In the random number generation method which generates a random number continuously when the essence of the above-mentioned example performs and feeds back the defined conversion based on the given initial value it is without changing the parameter which controls this conversion method before outputting only the random number sequence which is required to determine [ controlling the conversion method in this conversion by the parameter given from the exterior especially ] a conversion method and changing this conversion method. It cannot be overemphasized that linearity and not only a nonlinear feedback shift register but various methods can be used as a random

number generation method so that clearly from this.

[0047] Although the case where it controls by the parameter given from the outside also about the conversion method in feedback transformation has been described it is also controllable by the parameter which compounded the parameter given from the outside and the parameter generated inside.

[0048] (Example 4) Drawing 4 shows the case where a shift register is not used as a procedure of generating a random number.

[0049]  $n$  registers of  $R_1$  which operates with the respectively same clock in this example –  $R_n$  it consists of  $m$  linear transform (un-) circuits of  $S_1$  which performs linear transform (un-) by the output from each register and the feedback output from the last register ( $R_n$ ) and is outputted to the following register –  $S_m$ .

[0050] The procedure of the random number generation by this example is followed for the following to pass (however procedure 3.4.5. is performed simultaneously).

[0051] 1. Set an initial value as each register respectively.

[0052] 2. each (un-) linear transform circuit of  $S_1 - S_m$  opts for linear transform (un-) according to the parameter given from the outside.

[0053] 3. Output the value of a rightmost register ( $R_n$ ) as a random number and consider it as the value of the register ( $R_1$ ) of a high order end.

[0054] 4. Each register holds the value in an input part at the same time it outputs the value currently held in 3.

[0055] 5. each (un-) linear transform circuit changes the value and the feedback output from  $R_n$  which were outputted from the front register by the linear transform (un-) for which it opted by 2. and outputs them to a next register.

[0056] 6. although 3.4.5. is repeated below in order to be unable to analyze the output random number sequence by a formula (2) change the parameter inputted into a linear transform (un-) circuit before becoming larger than the number of the random numbers which the number of the random numbers outputted needs for the analysis of the random number sequence and change a linear transform (un-) method.

[0057] In this procedure all or a part of output of  $R_n$  serves as a random number generated by this example.

[0058] in the above-mentioned procedure the above-mentioned ROM etc. can constitute each (un-) linear transform circuit and each (un-) linear transform circuit may perform different (un-) linear transform respectively.

[0059] (Example 5) Drawing 5 shows the example in the case of using a DES (Data Encryption Standard) encryption circuit to the pseudo random number generator. It is possible that the leading decoding method called the difference decoding method these days is proposed there arises a question in the safety of a DES code and a key is frequently changed as the measure. When using a DES encryption circuit changing the key of a DES code will change a conversion method.

[0060] (Example 6) According to the following examples it has the parameter calculation circuit which used the method B in order to compute the parameter given

to the random number generator using the above-mentioned method A. By controlling the conversion method in a random number generator by the parameter outputted from this parameter calculation circuit, generating of the random number sequence which realizes two advantages, the rapidity which is an advantage of the method A and the safety which is the advantages of the method B is enabled as follows.

[0061] By changing the value of said tap sequence in the neighborhood which becomes equal and making the method of conversion of a random number generation means change before the number of the random numbers outputted to the random number generator by the method A becomes larger than the number of random numbers required for the analysis of the random number sequence. It prevents from analyzing the output random number sequence by the method of a formula (2) and the safety of an output random number series can be improved. Therefore it controls by the method B by using the value of the tap sequence as a parameter.

[0062] In this case, since calculation of the parameter by the method B by the time it becomes larger than the number of the random numbers which the number of the random numbers outputted by the random number generator using the method A needs for the analysis of that random number sequence should just be performed even if the method B is in calculable at high speed, it is possible to generate a random number at high speed as a whole.

[0063] Even if it changes the value of the aforementioned tap sequence after outputting a sufficient number to analyze by the method of a formula (2) of random numbers, it is analyzable only at the time of the value of the tap sequence. And since control of the value of a tap sequence is performed by the method B, it is difficult to predict the value of the following tap sequence and since it can prevent analyzing all the random number series after it like before, it is safe after changing the value of a tap sequence.

[0064] (Example 7) Although the number of random numbers required for the analysis of an output random number series is twice the number of stages of LFSR in the random number generator by LFSR when a nonlinear feedback shift register is used, it is possible to make the number of random numbers required for analysis large beyond [ of LFSR ] a case. Therefore, since the number of bits required for the analysis of the output random number sequence by a formula (2) increases, there is an advantage that the calculated cycle of the parameter for changing the method of nonlinear transformation can be enlarged. It becomes a big advantage especially that a calculated cycle can be enlarged when using the difficult method B of high speed processing for a parameter calculation section.

[0065] The example using the nonlinear feedback shift register is shown in drawing 8. Drawing 8 is a block diagram showing the random number sequence generator at the time of using the nonlinear feedback shift register by this invention. It is constituted using the parameter calculation circuit 61 based on the method B using the nonlinear transformation circuit 21 which carries out nonlinear transformation of the value from

each register of a shift register and a shift register as a random number generation means based on the method A and is fed back to a shift register. A nonlinear transformation method is controlled by the output from the parameter calculation circuit 61.

[0066] The random number generation procedure by this example is followed for the following to pass (however procedure 4.5.6. is performed simultaneously).

[0067] 1. Set an initial value as each register and parameter calculation circuit of a shift register.

[0068] 2. A parameter calculation circuit computes the first parameter from the given initial value and outputs it to the nonlinear transformation circuit 21.

[0069] 3. The nonlinear transformation circuit 21 opts for nonlinear transformation according to the parameter given by 2.

[0070] 4. Each register shifts the given value to the right.

[0071] 5. Output the value of a rightmost register as a random number.

[0072] 6. Carry out feedback transformation of the value of each register according to the nonlinear transformation for which it opted by 3. and consider it as the value of the register of a high order end.

[0073] 7. Although 4.5.6. is repeated below in order to be unable to analyze the output random number sequence by a formula (2) before becoming larger than the number of the random numbers which the number of the random numbers outputted needs for the analysis of the random number sequence a parameter calculation circuit computes the following parameter outputs it to the nonlinear transformation circuit 21 and changes a nonlinear transformation method.

[0074] In this procedure all or a part of output of a nonlinear transformation circuit serves as all the values outputted by procedure 5. or a random number generated by this invention in part. It is realizable by ROM etc. which made correspondence of input and output of a publicly known nonlinear function memorize as composition of the concrete nonlinear transformation circuit 21.

[0075] (Example 8) In Examples 6 and 7 in order to explain this invention plainly considered it as the random number generation means and described the example using linearity and a nonlinear feedback shift register but. There is essence of this invention in controlling the conversion method of the random number generation means which used the method A by the parameter outputted from the parameter calculating means using the method B. It is in changing this conversion method with the output from a parameter calculating means before outputting only the random number sequence which is required to determine especially the conversion method of a random number generation means. It cannot be overemphasized that linearity and not only a nonlinear feedback shift register but various methods can be used as a random number generation means so that clearly from this.

[0076] To the pseudorandom-numbers evolution method safe in cryptography which can be used as the method B. The thing using RSA cryptograph discrete logarithm and



a reciprocal code is known as shown in literature "code and information security" (TsujiiAkira Kasaharathe 1990 issue\*\*\*\*Inc. Co.86 pages) other than a formula (3). These can also be used for the algorithm of the parameter calculating means of this invention.

[0077]Also when a pseudorandom-numbers evolution method and the contents safe in cryptography combine the method of using in feedback ROM made secretlike drawing 2the parameter generating means based on the method B can be constituted.

[0078]Since the contents cannot know the remaining values inside ROM from the value which generated by then ROM made secret from the ROM only by the method of using in feedbackthe parameter generating means based on the method B can be constituted.

[0079]Although the case where it controls only by the parameter generated by the parameter calculation circuit also about control of the conversion method of a random number generation means has been describedIt is also controllable by the parameter which compounded the parameter inside a random number generation meansand the parameter computed in the parameter calculation circuit.

[0080](Example 9) Drawing 9 shows the case where a shift register is not used as a procedure of generating a random number.

[0081]In this example. As a random number generation means based on the method A. m of  $T_1$  which performs linear transform (un-) by the output from s registers and each register of  $R_1$  which operates with the respectively same clock -  $R_s$  and the feedback output from the last register ( $R_s$ ) and is outputted to the following register -  $T_m$ . (un-) it is constituted using the parameter calculation circuit 61 based on the method B using a linear transform circuit. each (un-) linear transform method is controlled by the output from the parameter calculation circuit 61.

[0082]The procedure of the random number generation by this example is followed for the following to pass (howeverprocedure 4.5.6. is performed simultaneously).

[0083]1. Resemble each register and the parameter calculation circuit 61 and set up an initial valuerespectively.

[0084]2. the parameter calculation circuit 61 computes the first parameter from the given initial valueand outputs it to each (un-) linear transform circuit.

[0085]3. each (un-) linear transform circuit of  $T_1 - T_m$  opts for each (un-) linear transform according to the parameter given by 2.

[0086]4. Output the value of a rightmost register ( $R_s$ ) as a random numberand consider it as the value of the register ( $R_1$ ) of a high order end.

[0087]5. Each register holds the value in an input part at the same time it outputs the value currently held in 4.

[0088]6. each (un-) linear transform circuit changes the value and the feedback output from  $R_s$  which were outputted from the front register by the linear transform (un-) for which it opted by 3. and outputs them to a next register.

[0089]7. Although 4.5.6. is repeated below in order to be unable to analyze the output random number sequence by a formula (2) before becoming larger than the number of the random numbers which the number of the random numbers outputted needs for the analysis of the random number sequence a parameter calculation circuit computes the following bar a meter outputs it to each (un-) linear transform circuit and changes each (un-) linear transform method.

[0090]In this procedure all or a part of output of  $R_s$  serves as a random number generated by this invention.

[0091]in the above-mentioned procedure the above-mentioned ROM etc. can constitute each (un-) linear transform circuit and each (un-) linear transform circuit may perform different (un-) linear transform respectively.

[0092](Example 10) Drawing 10 shows the example in the case of using the DES (Data Encryption Standard) encryption circuit 51 for a random number generation means in this invention. It is possible that the leading decoding method called the difference decoding method these days is proposed there arises a question in the safety of a DES code and a key is frequently changed as the measure. When using the DES cryptogram decoders 51 changing the key of a DES code will change a conversion method.

[0093](Example 11) Since the random number generated by the above-mentioned random number generator is strong to analysis as stated so far strong encryption communication with high safety is realizable to analysis by using this random number for a cipher system. Hereafter in the encryption communication network by the cipher system (stream cipher) which takes exclusive OR for every bit between correspondence and a random number the example of the encryption communication using a random number generator is shown.

[0094]The common key encryption system communication network which is sharing the encryption key peculiar [ drawing 11 ] among network members and secret is shown ABC--the encryption key that shares N between the member of the network  $K_{AB}$  and  $K_{AC}$  and -- is sharing between member A-B respectively the encryption key currently shared between member A-C and -- are shown.

[0095]Drawing 12 is a block diagram showing the composition of the communication apparatus 122 containing the cryptogram decoders and the decoding device at the time of using the random number generator 121 which consists of a random number generation circuit by this invention and a parameter calculation circuit.

[0096]Drawing 13 shows the situation of the secrecy communication between A in the cipher communication system shown by drawing 11 and drawing 12 and B.

[0097]Encryption communication to the member B is performed in the following procedures from the member A.

[0098]1. The communicative sending person A sets up all or a part of secret key  $K_{AB}$  currently shared with the transmission destination B as an initial value of a random number generation circuit and a parameter calculation circuit and generates random

number series  $k_i$ .

[0099]2. A takes exclusive OR for random number series  $k_i$  and correspondence  $m_i$  which were generated for every bit and is a cryptogram. [0100]

[External Character 3]

It calculates and the cryptogram is transmitted to B.

[0101]3. The communicative addressee B sets up all or a part of secret key  $K_{AB}$  currently shared the transmitting agency A as an initial value of a random number generation circuit and a parameter calculation circuit and generates the same random number series  $k_i$  as the sending person occurred.

[0102]4. B takes exclusive OR for random number series  $k_i$  and receiving cryptogram  $c_i$  which were generated for every bit and is correspondence. [0103]

[External Character 4]

It restores.

[0104]If this procedure is followed the cryptogram received since the regular transmission destination B knew that secret key  $K_{AB}$  can be decoded to original correspondence and since the other member (C-N) does not know the secret key used when carrying out that cryptogram he cannot know those contents. Secrecy communication is realized by this. The encryption key is not beforehand distributed like drawing 11 and also in the network of the gestalt which precedes performing encryption communication and needs to share an encryption key among transceiver persons if a common key is performed by a publicly known technique encryption communication is realizable in the same procedure.

[0105](Example 12) Since the encryption communication network shown in Example 11 is sharing the key peculiar between the sending person and addressee of correspondence and secret Receiving the cryptogram that it can decode to the correspondence which makes a meaning has guaranteed to the addressee that correspondence was transmitted by the owner of one more person who is the key. Therefore in the secrecy communications system shown in Example 11 attestation of a communicative addresser and an action addressee can also be performed.

[0106](Example 13) The encryption key is not beforehand distributed like Examples 11 and 12 In the network of the gestalt which precedes performing encryption communication and needs to share an encryption key among transceiver persons As a method which can share an encryption key safely even when the possible channel of tapping is passed. The method (W. Diffie and M.E. Hellman "New Directions in cryptography" IEEE IT and vol. I.T-22 No.6-1976) of Diffie-Hellman is known well. The random number by which it was generated by this invention can be used as a random number used in that case.

[0107]In that casesince the random number to be used does not need to have the same thing by the sending person and an action addresseethe initial value set as a random number generation means and a parameter generating means should just use any value.

[0108]

[Effect of the Invention]As explained abovebefore the number of the random numbers outputted from a fixed number of power range system sequences by the method (method A) in which analysis is possible becomes larger than a number required for the analysisby this inventionthe parameter of the method A is changed in the neighborhood which becomes equal.

Thereforeit is effective in it becoming difficult to collect a number required for the analysis of the method A of outputsand the safety of the random number by which it is generated being improved.

[0109]It is effective in the safety of the method A being improved further by changing the parameter of the method A based on the random number outputted by a method (method B) with difficult analysis from a power range system sequence.

[0110]In this casesince the output of the random number by the method B by the time it becomes larger than the number which the number of the outputs outputted from the method A needs for the analysis of the method A should just be performedit cannot be necessary to perform the random number generation of the method B at high speed. Howeversince the final output is an output from the method Ait can generate a random number at high speed.

[0111]If this random number series is used for encryption communicationit is effective in encryption communication with high high speed and safety being realized.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1]It is a figure showing the block configuration of the random number generator using LFSR.

[Drawing 2]It is a figure showing the detailed block configuration of the random number generator using LFSR.

[Drawing 3]It is a figure showing the block configuration of the random number generator using a nonlinear feedback register.

[Drawing 4]It is a figure showing the block configuration of the random number generator using two or more registers.

[Drawing 5]It is a figure showing the block configuration of the random number generator using DES cryptogram decoders.

[Drawing 6]It is a figure showing the block configuration of the random number

generator using LFSR.

[Drawing 7] It is a figure showing the block configuration of the random number generator using LFSR.

[Drawing 8] It is a figure showing the block configuration of the random number generator using a nonlinear feedback register.

[Drawing 9] It is a figure showing the block configuration of the random number generator using two or more registers.

[Drawing 10] It is a figure showing the block configuration of the random number generator using DES cryptogram decoders.

[Drawing 11] It is a figure explaining a common key cryptosystem communication network.

[Drawing 12] It is a block diagram showing the composition of the communication apparatus containing cryptogram decoders and a decoding device.

[Drawing 13] It is a figure explaining the communications system which performs secrecy communication.

[Drawing 14] It is a figure showing the block configuration of the conventional random number generator using LFSR.

[Description of Notations]

11 Shift register

12 Linear transform circuit

21 Register

31 Nonlinear transformation circuit

51 DES encryption circuit

61 Parameter calculation circuit

71 ROM

72 Buffer

73 a square -- a remainder operation circuit

121 Random number generator

122 Communication apparatus

---